F.#2019R00929

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----------X

UNITED STATES OF AMERICA 20-CR-442 (EK)

v.

BAIMADAJIE ANGWANG,

Defendant.

----------X

THE GOVERNMENT'S ~~CLASSIFIED~~ MEMORANDUM IN OPPOSITION TO THE DEFENDANT'S MOTION FOR NOTICE, DISCLOSURE, AND SUPPRESSION

BREON PEACE
United States Attorney
Eastern District of New York

J. Matthew Haggans
Francisco J. Navarro
Assistant United States Attorneys
Eastern District of New York

Scott A. Claffee
Trial Attorney
National Security Division
U.S. Department of Justice
Special Assistant U.S. Attorney
Eastern District of New York

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Federal Cases

U.S. Constitution

Federal Statutes

Other Authorities

I. INTRODUCTION

The Government is filing this unclassified memorandum in opposition to defendant Baimadajie Angwang's "Motion for Notice, Disclosure, and Suppression, Pursuant to 50 U.S.C. 1806" (hereinafter, the "defendant's motion"). (Docket Number ("Dkt.") 86.) The defendant's motion seeks an order: "1) directing the Government to provide notice and discovery of any surveillance obtained or derived pursuant to the Foreign Intelligence Surveillance Act, (50 U.S.C. 1806(c)); and 2) suppression pursuant to 50 U.S.C. 1806(e) on the grounds that the information was unlawfully acquired; or the surveillance was not made in conformity with an order of authorization or approval." (Dkt 86, at 1.)

The defendant's motion has triggered this Court's review of the application(s), order(s), and other materials related to the FISA-authorized electronic surveillance and physical search (*i.e.*, "the FISA materials")[1] to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search was made in conformity with an order of authorization or approval.[2] FISA specifies:

> [W]henever a motion is made pursuant to subsection (e) . . . to discover or obtain applications or orders or other materials relating to electronic surveillance [or physical search] or to discover, obtain, or suppress evidence or information obtained or derived

---

[1] **[CLASSIFIED INFORMATION REDACTED]**

[2] The provisions of FISA that address electronic surveillance are found at 50 U.S.C. §§ 1801-1812; those that address physical search are found at 50 U.S.C. §§ 1821-1829. These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision. This memorandum references the statutory language in effect at the time relevant to this matter.

Although the defendant's motion only cites to the FISA provisions addressing electronic surveillance, the defendant was also notified that the Government intends to use information obtained or derived from physical search under FISA. Therefore, this brief also discusses such physical search.

> from electronic surveillance [or physical search] under this Act, the United States district court . . . shall . . . if the Attorney General[3] files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or search] as may be necessary to determine whether the surveillance [or search] of the aggrieved person was lawfully authorized and conducted.

50 U.S.C. §§ 1806(f), 1825(g). The Government is filing herewith such an affidavit.[4] Consequently, the Government respectfully submits that, for the reasons set forth herein, this Court must conduct an *in camera, ex parte* review of the documents relevant to the defendant's motion in accordance with the provisions of 50 U.S.C. §§ 1806(f) and 1825(g).[5]

The Government respectfully submits that, for the reasons set forth below, and as the Court's *in camera, ex parte* review will show: (1) the electronic surveillance and physical search at issue in this case were both lawfully authorized and lawfully conducted in compliance with FISA; and (2) disclosure to the defendant of the FISA materials and the Government's classified submissions is not authorized because the Court can make an accurate determination of the legality of the FISA-authorized electronic surveillance and physical search without disclosing the FISA materials or portions thereof. Additionally, insofar as the defendant contemplates a future argument that the FISA information should be suppressed, the Government respectfully submits that no such suppression is warranted, and the FISA information should not be suppressed.

---

[3] As defined in FISA, "Attorney General" means the Attorney General of the United States (or Acting Attorney General), the Deputy Attorney General, or, upon the designation of the Attorney General, the Assistant Attorney General for National Security (AAG/NS). *See* 50 U.S.C. §§ 1801(g) and 1821(1). Such designation was made by then-Attorney General Eric. H. Holder, Jr., on April 24, 2009.

[4] The Declaration and Claim of Privilege, an affidavit executed by the AAG/NS, is filed both publicly and as an exhibit in the Sealed Appendix to the classified filing. *See* Sealed Exhibit 1.

[5] **[CLASSIFIED INFORMATION REDACTED]**

A. BACKGROUND

[CLASSIFIED INFORMATION REDACTED][6]

On September 19, 2020, a criminal complaint was sworn against Angwang, and the FBI arrested the defendant pursuant to that complaint on September 21, 2020. (Dkt. 1).[7]

On October 13, 2020, a grand jury in the Eastern District of New York returned an indictment charging Angwang with one count of acting as an agent of a foreign government without prior notification to the Attorney General, in violation of 18 U.S.C. § 951(a); one count of wire fraud, in violation of 18 U.S.C. § 1343; one count of making false statements, in violation of 18 U.S.C. § 1001(a)(3); and one count of obstruction of an official proceeding, in violation of 18 U.S.C. § 1512(c)(2). (Dkt. 20).

On October 30, 2020, the Government provided notice to this court and Angwang that it intends to offer into evidence or otherwise use or disclose information obtained or derived from electronic surveillance and physical search conducted pursuant to FISA. *See* 50 U.S.C. §§ 1806(c), 1825(d). (Dkt. 25).

[CLASSIFIED INFORMATION REDACTED]

On February 2, 2022, the defendant filed his motion. (Dkt. 86). Trial is set for September 12, 2022.

[CLASSIFIED INFORMATION REDACTED]

---

[6] As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

[7] **[CLASSIFIED INFORMATION REDACTED]**

B. OVERVIEW OF THE FISA AUTHORITIES

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. The Foreign Intelligence Surveillance Court's Findings

[CLASSIFIED INFORMATION REDACTED]

II. THE FISA PROCESS

A. OVERVIEW OF FISA

Enacted in 1978, and subsequently amended, FISA authorizes the Chief Justice of the United States to designate eleven United States District Judges to sit as judges of the Foreign Intelligence Surveillance Court (FISC). 50 U.S.C. § 1803(a)(1). The FISC judges are empowered to consider *ex parte* applications submitted by the Executive Branch for electronic surveillance and physical search when a significant purpose of the application is to obtain foreign intelligence information, as defined in FISA. Rulings of the FISC are subject to review by the Foreign Intelligence Surveillance Court of Review ("FISC of Review"), which is composed of three United States District or Circuit Judges who are designated by the Chief Justice. 50 U.S.C. § 1803(b).

As originally enacted, FISA required that a high-ranking member of the Executive Branch of Government certify that "the purpose" of the FISA application was to obtain foreign intelligence information. In 2001, FISA was amended as part of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

("USA PATRIOT Act").[8] One change to FISA accomplished by the USA PATRIOT Act is that a high-ranking official is now required to certify that the acquisition of foreign intelligence information is "a significant purpose" of the requested surveillance. See 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B).

FISA provides that the Attorney General may authorize the emergency employment of electronic surveillance and physical search if the Attorney General makes certain determinations set forth in the statute. *See* 50 U.S.C. §§ 1805(e)(1), 1824(e)(1).[9] Emergency electronic surveillance or physical search must comport with FISA's minimization requirements, which are discussed below. 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).

B. THE FISA APPLICATION

FISA provides a statutory procedure whereby the Executive Branch may obtain a judicial order authorizing the use of electronic surveillance and/or physical search within the United States where a significant purpose is the collection of foreign intelligence information.[10] 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B). Under FISA, foreign intelligence information is defined as:

> (1) information that relates to, and if concerning a United States person[11] is necessary to, the ability of the United States to protect against–
>
> > (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

---

[8] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[9] **[CLASSIFIED INFORMATION REDACTED]**

[10] **[CLASSIFIED INFORMATION REDACTED]**

[11] **[CLASSIFIED INFORMATION REDACTED]**

> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e); *see also id.* § 1821(1) (adopting the definitions from 50 U.S.C. § 1801). With the exception of emergency authorizations, FISA requires that a court order be obtained before any electronic surveillance or physical search may be conducted.

An application to conduct electronic surveillance pursuant to FISA must contain, among other things:

> (1) the identity of the federal officer making the application;
>
> (2) the identity, if known, or a description of the specific target of the electronic surveillance;
>
> (3) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
>
> (4) a statement of the proposed minimization procedures to be followed;
>
> (5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
>
> (6) a certification, discussed below, of a high-ranking official;
> (7) a summary of the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;

> (8) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
>
> (9) the proposed duration of the electronic surveillance.

50 U.S.C. § 1804(a)(1)-(9).

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance except that an application to conduct a physical search must also contain a statement of the facts and circumstances that justify an applicant's belief that "the premises or property to be searched contains foreign intelligence information" and that each "premises or property to be searched is or is about to be, owned, used, possessed by, or is in transit to or from" the target. *Id.* §§ 1823(a)(1)-(8), (a)(3)(B), (C).

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking Executive Branch official with national security responsibilities that:

> (A) the certifying official deems the information sought to be foreign intelligence information;
>
> (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
>
> (C) such information cannot reasonably be obtained by normal investigative techniques;
>
> (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
>
> (E) includes a statement of the basis for the certification that –
>
> > (i) the information sought is the type of foreign intelligence information designated; and
> >
> > (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(6); *see also id.* § 1823(a)(6).

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical search, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

> reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. §§ 1801(h)(1), 1821(4)(A).

In addition, minimization procedures also include "procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(c).

[CLASSIFIED INFORMATION REDACTED]

3. Attorney General's Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical search, or both, before they are presented to the FISC.

C. THE FISC'S ORDERS

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical search, or both, only upon finding, among other things, that:

(1) the application has been made by a "Federal officer" and has been approved by the Attorney General;

(2) there is probable cause to believe that (A) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (B) the facilities or places at which the electronic surveillance is directed are being used, or are about to be used, by a foreign power or an agent of a foreign power, or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the statutory requirements set forth in section 1801(h) (electronic surveillance) and section 1821(4) (physical search);

(4) the application contains all of the statements and certifications required by section 1804 (electronic surveillance) or section 1823 (physical search); and

(5) if the target is a United States person, the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines "foreign power" to mean –

(1) a foreign government or any component, thereof, whether or not recognized by the United States;

(2) a faction of a foreign nation or nations, not substantially composed of United States persons;

(3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of United States persons;

(6) an entity that is directed and controlled by a foreign government or governments; or

(7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

50 U.S.C. § 1801(a)(1)-(7); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

"Agent of a foreign power" means –

(1) any person other than a United States person, who—

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4);

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

(C) engages in international terrorism or activities in preparation therefore [sic];

(D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or

(E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor, for or on behalf of a foreign power; or

(2) any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

> (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or
>
> (E) knowingly aids or abets any person in the conduct of activities described in subparagraphs (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraphs (A), (B), or (C).

50 U.S.C. § 1801(b)(1) and (2); *see also id.* § 1821(1) (adopting definitions from 50 U.S.C. § 1801).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A). Although protected First Amendment activities cannot form the sole basis for FISA-authorized electronic surveillance or physical search, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. Aug. 18, 1994), *aff'd*, 189 F.3d 88 (2d Cir. 1999); *United States v. Rosen*, 447 F. Supp. 2d 538, 548-49 (E.D. Va. Aug. 14, 2006). The FISA application must establish probable cause to believe the target is acting as an agent of a foreign power at the time of the application. *See United States v. Turner*, 840 F.3d 336, 340-41 (7th Cir. 2016) (finding probable cause that the target of the FISA collection was an agent of a foreign power); *United States v. Squillacote*, 221 F.3d 542, 554 (4th Cir. 2000) (concluding that the FISA applications established "probable cause to believe that . . . [the targets] were agents of a foreign power at the time the applications were granted"); *United States v. Abu-Jihaad*, 531 F. Supp. 2d 299, 310 (D. Conn. Jan. 24, 2008) (finding that the FISA collection was lawfully collected and finding specifically, *inter alia*, that "[e]ach application contained facts establishing probable cause to believe that, at

the time the application was submitted to the FISC, the target of the FISA collection was an agent of a foreign power . . . ."), *aff'd*, 630 F.3d 102 (2d Cir. 2010); *Global Relief Found. Inc. v. O'Neill*, 207 F. Supp. 2d 779, 790 (N.D. Ill. June 11, 2002) (concluding that "the FISA application established probable cause . . . at the time the search was conducted and the application was granted"), *aff'd*, 315 F.3d 748 (7th Cir. 2002). However, FISA provides that "[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC has made all of the necessary findings and is satisfied that the FISA application meets the statutory provisions, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical search, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

> (1) the identity, if known, or a description of the specific target of the collection;
>
> (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
>
> (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;
>
> (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;
>
> (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and
>
> (6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1), (2)(A), 1824(c)(1), (2)(A).

Under FISA, electronic surveillance targeting a United States person may be approved for up to 90 days, except that electronic surveillance targeting a foreign power as defined in 50 U.S.C. § 1801(a)(1), (2), or (3) may be approved for up to one year, and that targeting a non-United States person agent of a foreign power may be approved for up to 120 days. 50 U.S.C. §§ 1805(d)(1), 1824(d)(1). Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. An extension for electronic surveillance or physical search targeting a United States person may be approved for up to 90 days, and one targeting a non-United States person or foreign power may be approved for up to one year. 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

III. DISTRICT COURT'S REVIEW OF FISC ORDERS

FISA authorizes the use in a criminal prosecution of information obtained or derived from any FISA-authorized electronic surveillance or physical search, provided that advance authorization is obtained from the Attorney General, 50 U.S.C. §§ 1806(b), 1825(c), and that proper notice is subsequently given to the court and to each aggrieved person[12] against whom the information is to be used. 50 U.S.C. §§ 1806(c)-(d), 1825(d)-(e). Upon receiving notice, an aggrieved person against whom the information is to be used may move to suppress the FISA information on two grounds: (1) the information was unlawfully acquired; or (2) the electronic surveillance or physical search was not conducted in conformity with an order of authorization or approval. 50 U.S.C. §§ 1806(e), 1825(f). In addition, FISA contemplates that a defendant may

[12] An "aggrieved person" is defined as the target of electronic surveillance or "any other person whose communications or activities were subject to electronic surveillance," 50 U.S.C. § 1801(k), as well as "a person whose premises, property, information, or material is the target of physical search" or "whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2). Angwang is an "aggrieved person" under FISA, and as noted above, was provided with notice of his status as such and of the government's intent to use FISA-obtained or -derived information against him at trial.

file a motion or request under any other statute or rule of the United States to discover or obtain applications, orders, or other materials relating to electronic surveillance, *i.e.*, the FISA materials. 50 U.S.C. §§ 1806(f), 1825(g).

A. THE REVIEW IS TO BE CONDUCTED *IN CAMERA* AND *EX PARTE*

In assessing the legality of FISA-authorized electronic surveillance and physical search, or both, the district court:

> shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[13]

50 U.S.C. §§ 1806(f), 1825(g). On the filing of such an affidavit or declaration as has been filed here by the AAG/NS, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance [or search]." 50 U.S.C. §§ 1806(f), 1825(g). Thus, the propriety of the disclosure of any FISA applications or orders to a defendant may not even be considered unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the acquired collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. *See Abu-Jihaad*, 630 F.3d at 129; *United States v. Duggan*, 743 F.2d 59, 78 (2d Cir. 1984) (After an *in-camera* review, the court "has the discretion to disclose portions of the

[13] **[CLASSIFIED INFORMATION REDACTED]**

documents, under appropriate protective procedures, only if [the judge] decides that such disclosure is 'necessary to make an accurate determination of the legality of the surveillance.'") (quoting 50 U.S.C. § 1806(f)); *United States v. Daoud*, 755 F.3d 479, 484 (7th Cir. 2014) ("Unless and until a district judge performs his or her statutory duty of attempting to determine the legality of the surveillance without revealing any of the fruits of the surveillance to defense counsel, there is no basis for concluding that disclosure is necessary in order to avert an erroneous conviction."); *United States v. Omar*, 786 F.3d 1104, 1110-11 (8th Cir. 2015) (citing *United States v. Isa*, 923 F.2d 1300, 1306 (8th Cir. 1991)); *United States v. El-Mezain*, 664 F.3d 467, 565 (5th Cir. 2011); *United States v. Hamide*, 914 F.2d 1147, 1149-50 (9th Cir. 1990) (upon review of the FISA materials, the court determined "that [disclosure] is not necessary, to the determination of the legality of the electronic surveillances submitted to the court to disclose those [FISA materials] to respondents"); *United States v. Ott*, 827 F.2d 473, 476 (9th Cir. 1987); *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982).

1. *In Camera, Ex Parte* Review Is the Rule

Federal courts, including the Second Circuit, have repeatedly and consistently held that FISA anticipates that an *ex parte*, *in camera* determination is to be the rule, while "[d]isclosure and an adversary hearing are the exception, occurring *only* when necessary." *Daoud*, 755 F.3d at 481 (finding that "the district judge must, in a non-public ('*in camera*'), nonadversarial ('*ex parte*') proceeding, attempt to determine whether the surveillance was proper"); *see also Duggan*, 743 F.2d at 78[14]; *El-Mezain*, 664 F.3d at 567 ("disclosure of FISA materials is the

[14] In *Duggan*, the Second Circuit explained that disclosure might be necessary "if the judge's initial review revealed potential irregularities such as 'possible misrepresentations of fact, vague identification of persons to be surveilled or surveillance records which include[] a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" 743 F.2d at 78 (quoting S. Rep. No. 95-701,

exception and *ex parte*, *in camera* determination is the rule") (citing *Abu-Jihaad*, 630 F.3d at 129); *Belfield*, 692 F.2d at 147; *accord Omar*, 786 F.3d at 1110 (quoting *Isa*, 923 F.2d at 1306); *Rosen*, 447 F. Supp. 2d at 546.

In fact, every court but one (whose decision was subsequently overturned by the Seventh Circuit)[15] that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera, ex parte* review. *See, e.g.*, *United States v. Stewart*, 590 F.3d 93 (2d Cir. 2009); *Abu-Jihaad*, 531 F. Supp. 2d at 310, *aff'd*, 630 F.3d at 129-30; *Omar*, 786 F.3d at 1110-11; *El-Mezain*, 664 F.3d at 566 (quoting district court's statement that no court has ever held an adversarial hearing to assist the court); *In re Grand Jury Proceedings of the Special Apr. 2002 Grand Jury ("In re Grand Jury Proceedings")*, 347 F.3d 197, 203 (7th Cir. 2003) (noting that no court has ever ordered disclosure of FISA materials); *Isa*, 923 F.2d at 1306 ("study of the materials leaves no doubt that substantial national security interests required the *in camera, ex parte* review, and that the district court properly conducted such a review"); *United States v. Alimehmeti*, No. 16 Cr. 398 (PAE) (S.D.N.Y. Sept. 22, 2017), Dkt. 68 at 6 (noting that *in camera, ex parte* determination of legality of FISA surveillance is "the rule" and finding that, because such a review "permitted the Court to make an accurate determination of the challenged surveillance . . . [d]isclosure and an adversary hearing are therefore not necessary" (internal

---

95th Cong., 2d Sess., at 11-12 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973).

[15] The district court in *United States v. Daoud*, No. 12-CR-723, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014), ruled that it was capable of making the determination, but nevertheless ordered the disclosure of FISA materials. The Government appealed the *Daoud* court's order to the U.S. Court of Appeals for the Seventh Circuit, which overturned the district court's decision to disclose, stating, "So clear is it that the materials were properly withheld from defense counsel that there is no need for a remand to enable the district judge to come to the same conclusion, because she would have to do so." *Daoud*, 755 F.3d at 485.

quotation marks omitted)); *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987); *Rosen*, 447 F. Supp. 2d at 546; *United States v. Sattar*, No. 02-CR-395, 2003 WL 22137012, at *6 (S.D.N.Y. Sept. 15, 2003) (citing *United States v. Nicholson*, 955 F. Supp. 588, 592 & n.11 (E.D. Va. Feb. 14, 1997)) (noting "this court knows of no instance in which a court has required an adversary hearing or disclosure in determining the legality of a FISA surveillance"); *United States v. Thomson*, 752 F. Supp. 75, 79 (W.D.N.Y. Oct. 24, 1990).

As the exhibits in the Sealed Appendix make clear, there is nothing extraordinary about the instant FISA-authorized electronic surveillance and physical search that would justify the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the electronic surveillance and physical search were made in conformity with an order of authorization or approval. In other words, the materials presented "are straightforward and readily understood." *In re Kevork*, 634 F. Supp. 1002, 1008 (C.D. Cal. Aug. 5, 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as in other cases, "[t]he determination of legality in this case is not complex." *Belfield*, 692 F.2d at 147; *Abu-Jihaad*, 531 F. Supp. 2d at 310; *United States v. Warsame*, 547 F. Supp. 2d 982, 987 (D. Minn. Apr. 17, 2008) (finding that the "issues presented by the FISA applications are straightforward and uncontroversial"); *Thomson*, 752 F. Supp. at 79. This Court, much like the aforementioned courts, is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

In addition to the specific harm that would result from the disclosure of the FISA materials in this case, which is detailed in the classified declaration of a high-ranking FBI official in support of the Declaration and Claim of Privilege of the AAG/NS, the underlying rationale for non-disclosure is clear: "In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized." *Ott*, 827 F.2d at 477 ("Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question.") (emphasis in original); *accord Isa*, 923 F.2d at 1306 (the Court's "study of the materials leaves no doubt that substantial national security interests required the *in camera, ex parte* review, and that the district court properly conducted such a review"); *United States v. Medunjanin*, No. 10-CR-19-1, 2012 WL 526428, at *9 (E.D.N.Y. Feb. 16, 2012) (finding persuasive the Government's argument that "unsealing the FISA materials in this case would provide the defense with unnecessary details of an extraordinarily sensitive anti-terrorism investigation"); *United States v. Islamic Am. Relief Agency ("IARA")*, No. 07-00087-CR-W-NKL, 2009 WL 5169536, at *3-4 (W.D. Mo. Dec. 21, 2009).

Confidentiality is critical to national security. "If potentially valuable intelligence sources" believe that the United States "will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information." *CIA v. Sims*, 471 U.S. 159, 175 (1985); *see also Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When considering whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of

weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) ("each individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself"). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would also create potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

> Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to "reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights." In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also Stewart*, 590 F.3d at 128 ("FISA applications are likely to contain allegedly sensitive information relating to perceived issues of national security. . . . For this reason, *ex parte*, *in camera* determination is to be the rule.")

(quoting *Duggan*, 743 F.2d at 77); *Daoud*, 755 F.3d at 483 ("Everyone recognizes that privacy is a legally protectable interest, and it is not an interest of private individuals alone. [FISA] is an attempt to strike a balance between the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation."); *ACLU Found. of So. Cal. v. Barr*, 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that 50 U.S.C. § 1806(f) "is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance").

2. *In Camera, Ex Parte* Review Is Constitutional

The constitutionality of FISA's *in camera, ex parte* review provisions has been affirmed by every federal court that has considered the matter. *See, e.g.*, *Stewart*, F.3d 590 at 126 (the Second Circuit has concluded that "the procedures fashioned in FISA [are] a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information") (quoting *Duggan*, 743 F. 2d at 73); *Abu-Jihaad*, 630 F.3d at 117; *El-Mezain*, 664 F.3d at 567; *Ott*, 827 F.2d at 476-77 (FISA's review procedures do not deprive a defendant of due process); *Belfield*, 692 F.2d at 148-49; *United States v. Damrah*, 412 F.3d 618, 624 (6th Cir. 2005) ("FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process."); *ACLU Found. of So. Cal.*, 952 F.2d at 465; *Isa*, 923 F.2d at 1306 (upholding the district court's *in camera, ex parte* review as constitutional and stating that the process delineated under FISA "provides even more protection" than defendants receive in other contexts); *United States v. Benkahla*, 437 F. Supp. 2d 541, 554 (E.D. Va. May 17, 2006); *United States v. Megahey*, 553 F. Supp. 1180, 1194 (E.D.N.Y. Dec. 1, 1982) ("*ex parte*, *in camera* procedures provided in 50 U.S.C. § 1806(f) are constitutionally sufficient to determine the lawfulness of the electronic

surveillance at issue while safeguarding defendant's fourth amendment rights"); *United States v. Falvey*, 540 F. Supp. 1306, 1315-16 (E.D.N.Y. June 15, 1982) (a "massive body of pre-FISA case law of the Supreme Court, [the Second] Circuit and others" supports the conclusion that the legality of electronic surveillance should be determined on an *in camera, ex parte* basis).

In summary, FISA mandates a process by which the district court must conduct an initial *in camera, ex parte* review of FISA applications, orders, and related materials in order to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval. Such *in camera, ex parte* review is the rule in such cases and that procedure is constitutional. In this case, the AAG/NS has filed the required declaration invoking that procedure and has declared that disclosure or an adversary hearing would harm national security. Accordingly, an *in camera, ex parte* review by this Court is the appropriate venue in which to determine whether the FISA information was lawfully acquired and whether the electronic surveillance and physical search were made in conformity with an order of authorization or approval.

B. THE DISTRICT COURT'S SUBSTANTIVE REVIEW

In evaluating the legality of the FISA collection, a district court's review should determine: (1) whether the certification submitted by the Executive Branch in support of a FISA application was properly made; (2) whether the application established the probable cause showing required by FISA; and (3) whether the collection was properly minimized. *See Abu-Jihaad*, 630 F.3d at 130-31; *see also* 50 U.S.C. §§ 1806(f), 1825(g).

1. Standard of Review of Probable Cause

Although federal courts are not in agreement as to whether the FISC's probable cause determination should be reviewed *de novo* or afforded due deference, courts in the Second Circuit, including in this District, have afforded due deference to the determinations of the FISC.[16] *See Abu-Jihaad*, 630 F.3d at 130 ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submissions in this case would easily allow it to clear a higher standard of review."); *Stewart*, 590 F.3d at 128; *Alimehmeti*, Dkt. 68 at 7; *United States v. Fishenko*, No. 12-CV-626 (SJ), 2014 WL 4804215, at *3 (E.D.N.Y. Sept. 25, 2014); *cf. Medunjanin*, 2012 WL 526428, at *6-7 (affording deferential review, but noting that such review is not superficial). The material under review here satisfies either standard of review. *See Omar*, 786 F.3d at 1112 ("[W]e have no hesitation in concluding that probable cause under FISA existed under any standard of review.")

2. Probable Cause Standard

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance or physical search is directed is being used, or is about to be used, is, or is about to be, owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power.

---

[16] Federal courts in other circuits have determined that the probable cause determination of the FISC should be reviewed *de novo*. *See United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *Turner*, 840 F.3d at 340 (in which a *de novo* review of the FISC's findings of probable cause was conducted); *Warsame*, 547 F. Supp. 2d at 990-91 (the required showing is "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability" that the search will be fruitful (citing *Illinois v. Gates*, 462 U.S. 231, 238 (1983))); *Rosen*, 447 F. Supp. 2d at 545. Even under the *de novo* standard, the Government believes that the Court would find that FISC's findings of probable cause were correct.

50 U.S.C. §§ 1805(a), 1824(a); *Abu-Jihaad*, 630 F.3d at 130. It is this standard — not the standard applicable to criminal search warrants — that this Court must apply. *See Abu-Jihaad*, 630 F.3d at 130-31; *Turner*, 840 F.3d at 340-41 (applying the FISA standard of probable cause rather than the probable cause in a criminal case); *Omar*, 786 F.3d at 1111 ("[R]ather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power.") (quoting *El-Mezain*, 664 F.3d at 564); *United States v. Duka*, 671 F.3d 329, 338 (3d Cir. 2011); *United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (citing *United States v. United States District Court (Keith)*, 407 U.S. 297, 322 (1972)).

[CLASSIFIED INFORMATION REDACTED]

The probable cause threshold, which the Government must satisfy before receiving authorization to conduct electronic surveillance or physical search under FISA, complies with the Fourth Amendment's reasonableness standard. The argument that FISA's different probable cause standard violates the Fourth Amendment's reasonableness requirement has been uniformly rejected by federal courts. *See, e.g.*, *Abu-Jihaad*, 630 F.3d at 120 (listing 16 cases that have ruled that FISA does not violate the Fourth Amendment).

The Supreme Court has stated that "[d]ifferent standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of the Government for intelligence information and the protected rights of our citizens." *Keith*, 407 U.S. at 322-23 (recognizing that domestic security surveillance "may involve different policy and practical considerations than the surveillance of 'ordinary crime'"). In *Keith*, the Supreme Court acknowledged that: (1) the "focus of . . . surveillance [in domestic security investigations] may be less precise than that directed against more conventional types of crime"; (2) unlike

ordinary criminal investigations, "[t]he gathering of security intelligence is often long range and involves the interrelation of various sources and types of information"; and (3) the "exact targets of such surveillance may be more difficult to identify" than in surveillance operations of ordinary crimes under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, (Pub. L. 90-351; 6/9/68) (Title III). *Id.* Although *Keith* was decided before FISA's enactment and addressed purely domestic security surveillance, the rationale underlying *Keith* applies *a fortiori* to foreign intelligence surveillance, where the Government's interest, at least from a national security perspective, would typically be more pronounced.

FISA was enacted partly in response to *Keith*. In constructing FISA's framework, Congress addressed *Keith*'s question of whether departures from traditional Fourth Amendment procedures "are reasonable, both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens," and "concluded that such departures are reasonable." *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., at 11-12 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3980. Similarly, many courts — including the Second Circuit and the FISC of Review — have relied on *Keith* in holding that FISA collection conducted pursuant to a FISC order is reasonable under the Fourth Amendment. *See Duggan*, 743 F.2d at 74 (holding that FISA does not violate the Fourth Amendment); *United States v. Ning Wen*, 477 F.3d 896, 898 (7th Cir. 2007) (holding that FISA is constitutional despite using "a definition of 'probable cause' that does not depend on whether a domestic crime has been committed"); *Damrah*, 412 F.3d at 625 (denying the defendant's claim that FISA's procedures violate the Fourth Amendment); *In re Sealed Case*, 310 F.3d 717, 738, 746 (FISA Ct. Rev. 2002) (finding that while many of FISA's requirements differ from those in Title III, few of those differences have constitutional relevance); *United States v. Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987) (finding

FISA's procedures compatible with the Fourth Amendment); *Cavanagh*, 807 F.2d at 790-91 (holding that FISA satisfies the Fourth Amendment requirements of probable cause and particularity); *Warsame*, 547 F. Supp. 2d at 993-94; *United States v. Mubayyid*, 521 F. Supp. 2d 125, 135-41 (D. Mass. Nov. 5, 2007) (rejecting claim that FISA violates the Fourth Amendment's judicial review, probable cause, notice, and particularity requirements); *United States v. Marzook*, 435 F. Supp. 2d 778, 786 (N.D. Ill. June 22, 2006) ("Courts uniformly have held that FISA procedures satisfy the Fourth Amendment's reasonableness requirement"); *Falvey*, 540 F. Supp. at 1311-14 (finding that FISA procedures satisfy the Fourth Amendment's warrant requirement).

3. Standard of Review of Certifications

Certifications submitted in support of a FISA application should be "subject only to minimal scrutiny by the courts," *Badia*, 827 F.2d at 1463, and are "presumed valid." *Duggan*, 743 F.2d at 77 & n.6 (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *see also Turner*, 840 F.3d at 342; *United States v. Campa*, 529 F.3d 980, 993 (11th Cir. 2008); *Rosen*, 447 F. Supp. 2d at 545; *Warsame*, 547 F. Supp. 2d at 990 ("a presumption of validity [is] accorded to the certifications"). When a FISA application is presented to the FISC, "[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information." *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should "have no greater authority to second-guess the executive branch's certifications than has the FISA judge." *Id.; see also In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Rahman*, 861 F. Supp. at 250.

The district court's review should determine whether the certifications were made in accordance with FISA's requirements. *See United States v. Omar*, No. 09-242, 2012 WL 2357734, at *3 (D. Minn. June 20, 2012), *aff'd*, 786 F.3d 1104 ("the reviewing court must presume as valid 'the representations and certifications submitted in support of an application for FISA surveillance' . . . absent a showing sufficient to trigger a *Franks* hearing"); *see also Campa*, 529 F.3d at 993 ("in the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target") (quoting *Badia*, 827 F.2d at 1463); *United States v. Alwan,* No. 1:11-CR-13, 2012 WL 399154, at *7 (W.D. Ky. Feb. 7, 2012) ("the [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made") (quoting *United States v. Ahmed*, No. 1:06-CR-147, 2009 U.S. Dist. LEXIS 120007, at *20 (N.D. Ga. Mar. 19, 2009). Under FISA, "[t]he FISA Judge need only determine that the application contains all of the statements and certifications required by the Act if the target is a non-United States person, whereas he must also find that the certifications are not 'clearly erroneous' if the target is a United States person." *Duggan*, 743 F.2d at 75; *Campa*, 529 F.3d at 994; *United States v. Kashmiri*, No. 09-CR-830, 2010 WL 4705159, at *2 (N.D. Ill. Nov. 10, 2010). A "clearly erroneous" finding is established only when "although there is evidence to support it, the reviewing court on the [basis of the] entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 WL 5169536, at *4 (identifying "clearly erroneous" standard of review for FISA certifications).

4. FISA Is Subject to the "Good Faith" Exception

Even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not met, the evidence obtained or derived from the FISA-authorized electronic surveillance and physical search is, nonetheless, admissible under the "good faith" exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984). Numerous courts have stated that the good faith exception applies to FISA evidence. *See Ning Wen*, 477 F.3d at 897 (noting that federal officers were entitled to rely in good faith on a FISA warrant); *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 ("[t]he FISA evidence obtained . . . would be admissible under *Leon*'s 'good faith' exception to the exclusionary rule were it not otherwise admissible under a valid warrant"); *Mubayyid*, 521 F. Supp. 2d at 140 n.12 ("there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders"); *Marzook*, 435 F. Supp. at 790-91 (holding, in an analogous context, that "the FBI's reliance on the Attorney General's approval under Executive Order No. 12333 – an order that no court has found unconstitutional – was [] objectively reasonable because that order pertains to foreign intelligence gathering").

In *Illinois v. Krull*, the Supreme Court "ruled categorically that 'suppressing evidence obtained by an officer acting in objectively reasonable reliance on a statute' would not further the purposes of the exclusionary rule, even if that statute is later declared unconstitutional." *Duka*, 671 F.3d at 346-37 (quoting *Krull*, 480 U.S. 340, 349-50 (1987)). The exclusionary rule should not be imposed to punish an officer who acts in objectively reasonable reliance on a duly enacted statute. "Because the rule 'is designed to deter police misconduct,' it applies only where it will 'alter the behavior of individual law enforcement officers or the policies of their

departments.'" *Duka*, 671 F.3d at 346 (quoting *Leon*, 468 U.S. at 916-18). Here, the exclusion of evidence would serve no such deterrent purpose. *See Davis v. United States*, 564 U.S. 229, 237 (2011); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 282-84 (S.D.N.Y. 2000).

In this case, there is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *Massachusetts v. Sheppard*, 468 U.S. 981, 987-88 (1984). Further, there are no facts indicating that the FISC failed to act in a neutral and detached manner in authorizing the electronic surveillance and physical search at issue. *See Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera, ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC's orders contained all of the requisite findings, and "well-trained officers" reasonably relied on those orders. Therefore, in the event that the Court questions whether a particular FISC order was supported by sufficient probable cause, the information obtained pursuant to that order would be admissible under *Leon*'s good faith exception to the exclusionary rule.

IV. THE FISA INFORMATION WAS LAWFULLY ACQUIRED AND THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE MADE IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED INFORMATION REDACTED]

A. THE INSTANT FISA APPLICATION(S) MET FISA'S PROBABLE CAUSE STANDARD

[CLASSIFIED INFORMATION REDACTED]

1. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

2. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

i. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

ii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

d. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

i. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

ii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

iii. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

3. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

c. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

d. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

4. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

a. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

b. [CLASSIFIED INFORMATION REDACTED]

[CLASSIFIED INFORMATION REDACTED]

B. THE CERTIFICATION(S) COMPLIED WITH FISA

[CLASSIFIED INFORMATION REDACTED]

1. Foreign Intelligence Information

[CLASSIFIED INFORMATION REDACTED]

2. "A Significant Purpose"

[CLASSIFIED INFORMATION REDACTED]

3. Information Not Reasonably Obtainable Through Normal Investigative Techniques

[CLASSIFIED INFORMATION REDACTED]

C. THE ELECTRONIC SURVEILLANCE AND PHYSICAL SEARCH WERE CONDUCTED IN CONFORMITY WITH AN ORDER OF AUTHORIZATION OR APPROVAL

[CLASSIFIED INFORMATION REDACTED]

1. The Minimization Procedures

Once a reviewing court is satisfied that the FISA information was lawfully acquired, it must then examine whether the electronic surveillance and physical search was lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(g). To do so, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

[CLASSIFIED INFORMATION REDACTED]

FISA's legislative history and the applicable case law demonstrate that the definitions of "minimization procedures" and "foreign intelligence information" were intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when "the investigation is focusing on what is thought to be a widespread conspiracy" and more extensive surveillance is necessary "to determine the precise scope of the enterprise." *In re Sealed Case*, 310 F.3d at 741; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. Dec. 5, 2000) ("more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted" [internal quotation marks omitted]). Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign

powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the "study" and to terrorist materials as "university papers"). As one court explained, "[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical." *Kevork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. 1, at 55 (1978)); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*, 310 F.3d at 740-41; *Thomson*, 752 F. Supp. at 81 (noting that it is permissible to retain and disseminate "bits and pieces" of information until the information's "full significance becomes apparent") (citing H.R. Rep. No. 95-1283, pt. 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, "individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time." *Rahman*, 861 F. Supp. at 252-53 (citing H.R. Rep. No. 95-1283, pt. 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *Mubayyid*, 521 F. Supp. 2d at 134; *Rahman*, 861 F. Supp. at 252. As a result, "courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information." *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need

to conduct a thorough post-acquisition review of FISA information that involves a United States person who is acting as an agent of a foreign power. As Congress explained:

> It is "necessary" to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

H.R. Rep. No. 95-1283, pt. 1, at 58. Indeed, at least one court has cautioned that, when a United States person communicates with an agent of a foreign power, the Government would be "remiss in meeting its foreign counterintelligence responsibilities" if it did not thoroughly "investigate such contacts and gather information to determine the nature of those activities." *Thomson*, 752 F. Supp. at 82.

In light of these realities, Congress recognized that "no electronic surveillance can be so conducted that innocent conversations can be totally eliminated." *See* S. Rep. No. 95-701, at 39 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4008 (quoting *United States v. Bynum,* 485 F.2d 490, 500 (2d Cir. 1973)). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the "mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance." 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an "objective assessment of the [agents'] actions in light of the facts and circumstances confronting [them] at the time." *Scott v. United States*,

436 U.S. 128, 136 (1978). "The test of compliance is 'whether a good-faith effort to minimize was made.'" *Mubayyid*, 521 F. Supp. 2d at 135; *see also Hammoud*, 381 F.3d at 334 ("[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information"); S. Rep. No. 95-701, at 39-40, 1978 U.S.C.C.A.N., at 4008-09 (stating that the court's role is to determine whether "on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion").

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is "evidence of a crime," whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (noting that "[t]here is no requirement that the 'crime' be related to foreign intelligence"). As a result, to the extent that certain communications of a United States person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See id.* at 1305.

Even if certain communications were not minimized in accordance with the SMPs, suppression would not be the appropriate remedy with respect to those communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff'd*, 500 F.2d 1401 (3d Cir. 1974) (discussing Title III). As discussed above, absent evidence that "on the whole" there has been a "complete" disregard for the minimization procedures, the fact that some communications should have been minimized does not affect the admissibility of others that were properly acquired and retained. FISA's legislative history reflects that Congress intended only a limited sanction for errors of minimization:

> As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

H.R. Rep. No. 1283, pt. 1, at 93; *see also Falcone*, 364 F. Supp. at 886-87; *Medunjanin*, 2012 WL 526428, at *12 (disclosure and suppression not warranted where "failure to adhere to [the minimization] protocol was *de minimis*").

2. The FISA Information Was Appropriately Minimized

[CLASSIFIED INFORMATION REDACTED]

Based upon this information, we respectfully submit that the Government lawfully conducted the FISA collection discussed herein. Consequently, for the reasons stated above, the Court should find that the FISA collection discussed herein was lawfully conducted under the minimization procedures approved by the FISC and applicable to the FISA collection discussed herein.

V. THE COURT SHOULD REJECT THE DEFENDANT'S LEGAL ARGUMENTS

A. The Defendant Has Not Established Any Basis for the Court to Disclose the FISA Materials

[CLASSIFIED INFORMATION REDACTED]

The defendant suggests that the "disclosure of any applications, affidavits or other materials relating to, the requests for and the granting of, electronic surveillance of [the defendant] under FISA," is necessary "[i]n order to determine whether the circumstances pertaining to the noticed surveillance give rise to a basis for suppression." (*See id.*) However, disclosure of the FISA materials to defense counsel is authorized only after the Court conducts its review of FISA materials *in camera* and *ex parte*, and only if the Court is unable to determine the legality of the electronic surveillance, physical search, or both, without the assistance of

defense counsel. *See* 50 U.S.C. §§ 1806(f), 1825(g); *Duggan*, 743 F.2d at 78; *Daoud*, 755 F.3d at 482; *In re Grand Jury Proceedings*, 347 F.3d at 203; *Rosen*, 447 F. Supp. 2d at 546. As the *Belfield* court stated: "Congress was adamant, in enacting FISA, that [its] 'carefully drawn procedure[s]' are not to be bypassed." 692 F.2d at 146 (citing S. Rep. No. 95-701, at 63). This holding is fully supported by the legislative history of 50 U.S.C. § 1806(f), which states: "The court may order disclosure to [the defense] only if it finds that such disclosure is necessary to make an accurate determination of the legality of the surveillance . . . . Once a judicial determination is made that the surveillance was lawful, a motion for discovery . . . must be denied." S. Rep. No. 95-701, at 64-65, 1978 U.S.C.C.A.N., at 4034. As this Court will see from its review, the FISA materials are presented in a well-organized and straightforward manner that will allow the Court to make its determination of the lawfulness of the FISA collection without input from defense counsel.

The defendant is not entitled to the FISA materials for the purpose of challenging the lawfulness of the FISA authorities, as FISA's plain language precludes defense counsel from accessing the classified FISA materials to conduct a fishing expedition. In *Medunjanin*, the court noted that "[d]efense counsel . . . may not inspect the FISA dockets to construct a better argument for inspecting the FISA dockets. Such a circular exercise would be patently inconsistent with FISA . . . ." 2012 WL 526428, at *10. *See also Badia*, 827 F.2d at 1464 (rejecting the defendant's request for "disclosure of the FISA application, ostensibly so that he may review it for errors"); *United States v. Mohamud*, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *32 (D. Or. June 24, 2014) ("Obviously it would be helpful to the court to have defense counsel review the materials prior to making arguments. Congress, however, did not put 'helpful' in the statute; it chose 'necessary.'"); *Mubayyid*, 521 F. Supp. 2d at 131.

[CLASSIFIED INFORMATION REDACTED]

The defendant has failed to present any colorable basis for disclosure, as this Court is able to review and make a determination as to the legality of the FISA collection without the assistance of defense counsel. Where, as here, defense participation is not necessary, FISA requires that the FISA materials remain protected from disclosure. Congress' clear intention is that FISA materials should be reviewed *in camera* and *ex parte* and in a manner consistent with the realities of modern intelligence needs and investigative techniques. There is simply nothing extraordinary about this case that would prompt this Court to order the disclosure of highly sensitive and classified FISA materials. *See Rosen*, 447 F. Supp. 2d at 546 ("exceptional nature of disclosure of FISA material is especially appropriate in light of the possibility that such disclosure might compromise the ability of the United States to gather foreign intelligence information effectively") (citing *Belfield*, 692 F.2d at 147).

B. The Defendant Has Not Established Any Basis for the Court to Suppress the FISA Information

As noted above, the defendant contemplates the need to first review the FISA materials before making an accurate determination of the legality of the surveillance (and perhaps then move to suppress some or all of the FISA information); however, the defendant did not argue that any FISA information should be suppressed at this time. Nevertheless, for the reasons discussed below, the Court should reject any future argument from the defendant to suppress the FISA information.

1. The Government Has Satisfied the Significant Purpose and Normal Investigative Techniques Standards

[CLASSIFIED INFORMATION REDACTED]

As part of the USA PATRIOT Act, Congress amended FISA to require that an Executive Branch official now certify that "a significant purpose" of the requested surveillance was to obtain foreign intelligence information. 18 U.S.C. § 1804(a)(6)(B). The "significant purpose" standard has been repeatedly upheld, including by the Second Circuit. As the Second Circuit observed in *Abu-Jihaad*, "we identify no constitutional infirmity in Congress's decision to allow FISA warrants to issue on certification of a 'significant purpose' to obtain foreign intelligence information. . . ." 630 F.3d at 131; *see also id.* at 128 (concluding that the standard "is sufficient to ensure that the executive may only use FISA to obtain a warrant when it is in good faith pursuing foreign intelligence gathering. . . ."); *Duka*, 671 F.3d at 343 ("the dispositive issue is whether the 'significant purpose' test is reasonable. . . . We agree with our sister courts of appeals and the Foreign Intelligence Surveillance Court of Review that the amended FISA's 'significant purpose' standard is reasonable under the Fourth Amendment.").

[CLASSIFIED INFORMATION REDACTED]

2. The Government Has Satisfied the Probable Cause Standard

[CLASSIFIED INFORMATION REDACTED]

As discussed above in § III.B , the probable cause threshold that the Government must satisfy before receiving authorization to conduct electronic surveillance and physical search under FISA complies with the Fourth Amendment's reasonableness standard. Arguments that FISA's different probable cause standard violates the Fourth Amendment have been uniformly rejected by federal courts. *See, e.g., Abu-Jihaad,* 630 F.3d at 120 (listing sixteen cases that have ruled FISA does not violate the Fourth Amendment).

3. The Government Complied with the Minimization Procedures

FISA requires that the Government comply with all applicable procedures to appropriately minimize information acquired pursuant to FISA. *See* 50 U.S.C. § 1805(a)(3).

[CLASSIFIED INFORMATION REDACTED]

VI. CONCLUSION: THERE IS NO BASIS FOR THE COURT TO DISCLOSE THE FISA MATERIALS OR SUPPRESS THE FISA INFORMATION

Based on the foregoing analysis, the Government respectfully submits that the Court must conduct an *in camera, ex parte* review of the FISA materials and the Government's classified submission, and should: (1) find that the electronic surveillance and physical search at issue in this case was both lawfully authorized and lawfully conducted in compliance with FISA; (2) hold that disclosure of the FISA materials and the Government's classified submissions to the defendant is not authorized because the Court is able to make an accurate determination of the legality of the electronic surveillance and physical search without disclosing the FISA materials or any portions thereof; (3) hold that the fruits of the electronic surveillance and physical search should not be suppressed; and (4) order that the FISA materials and the Government's classified submissions be maintained under seal by the Classified Information Security Officer or his or her designee.

A district court order granting motions or requests under 50 U.S.C. §§ 1806(g) or 1825(h), a decision that electronic surveillance or physical search was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is each a final order for purposes of appeal. See 50 U.S.C. §§ 1806(h), 1825(i). Should the Court conclude that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an

appeal. Accordingly, the Government respectfully requests that the Court stay any such order pending an appeal by the United States of that order.

Dated: Brooklyn, New York
March 17, 2022

Respectfully Submitted,

BREON PEACE
United States Attorney
Eastern District of New York

By: /s/
J. Matthew Haggans
Francisco J. Navarro
Assistant U.S. Attorneys
Eastern District of New York

Scott A. Claffee
Trial Attorney
National Security Division
U.S. Department of Justice
Special Assistant U.S. Attorney
Eastern District of New York